RFID: Frequency, standards, adoption and innovation

Matt Ward
Department of Design
Goldsmiths College, University of London

Rob van Kranenburg
Resonance Design/Virtueel Platform

Managing Author: Gaynor Backhouse, JISC TechWatch

This report was peer reviewed by:

William Marsterson
Pro Vice-Chancellor and Head of Learning Resources
Middlesex University

Alan Hopkinson
Head of Library Systems and Bibliographical Services
Middlesex University

Alex Birchall
Deputy Systems Librarian
Middlesex University

Kevin Kelly
Marketing Manager
RFID Centre
Bracknell
Berkshire

CONTENTS

EXECUTIVE SUMMARY

At the very simplest level, Radio Frequency Identification (RFID) technologies allow the transmission of a unique serial number wirelessly, using radio waves. The two key parts of the system that are needed to do this are the RFID 'tag' and the 'reader'; attaching an RFID tag to a physical object allows the object to be 'seen' and monitored by existing computer networks and back-office administration systems.

So far, the key driver for the development of RFID systems has been the desire to improve efficiency in globalised supply chains but implementation of the technology has been problematic. This is partly due to the manufacturing costs of tags, which are currently too high to justify widespread deployment across supply chains in the way that was originally imagined, and partly due to concerns over the potential for infringing the privacy of consumers who purchase RFID-tagged products. In addition, there are concerns about the health implications for staff employed in RFID-enabled workplaces, although this has not received as much attention in the press.

One of the areas where RFID has been a cost effective deployment is within library systems, where, due to the high value of individual books and journals and the many ways in which each tag can deliver value (e.g. issue/returns, stocktaking etc.), the one-off cost of a tag is easily off-set by overall cost savings and efficiency gains. However, there is a second key significance for RFID technologies: RFID tags are capable of providing the technological 'glue' to join physical objects to computer networks, and this is an important part of the technological jigsaw that will enable the 'seamless' and 'calm' technology vision of ubiquitous computing. A key milestone in this development is the realisation of the Internet of Things, where increasingly large numbers of our everyday objects and gadgets will have some kind of simple communication technology embedded into them, allowing them to be connected to each other within local networks and, ultimately, connected to the wider network of networks – the Internet.

There are various ways in which RFID may impact on the core business of Further and Higher Education (F&HE) but in the short term, one of the critical factors will be how concerns about the potential for privacy infringement are reduced. Although these concerns have not had as high a profile in the UK as they have elsewhere, pressure from the EU will require UK F&HE to start addressing these issues, and it will ultimately be more cost effective and time efficient if this is done in a pro-active rather than a re-active way. The influence of the library sector, in its dual role as a public sector body acting in the 'public good' and working as a test-bed for the technology, has the potential to be important in setting the pace for establishing good practice in this area while the technology is still relatively new and there is still the opportunity to have an impact.

1. INTRODUCTION

The history of RFID (Radio Frequency Identification) can be tracked as far back as the 1920s with the birth of radar systems (the word radar is an acronym for *ra*dio *d*etection *a*nd *r*anging). The development of the technology, a combination of radar and radio broadcast technology, is messy and convoluted but there is consensus that it developed from the work carried out during WW2 to identify enemy aircraft, known as 'Identification: Friend or Foe' (IFF) systems.

1.1 What is RFID? The basics

An RFID system has two main components: the RF reader (known also as the base-station or interrogator) and the RF tag (or transponder). When RFID tags are attached to physical objects they enable those objects to identify themselves to RFID readers through the use of radio frequency communication.

In principle, and on the very simplest level, RFID tags allow objects to say, “Hello, I’m here and my name is …”. When discussing digital ‘intelligence’ with regard to an object or environment we have to keep in mind that although there are different sorts of tags with different levels of computing capability, the main intelligence resides in the network or application connected to the RFID system. The main purpose of an RFID tag is to act as 'glue' to a digitally mediated world.

1.1.1 The Tag

There are two main components present in the RFID tag. Firstly, a small silicon chip or integrated circuit which contains a *unique* identification number (ID). Secondly, an antenna that can send and receive radio waves. These two components can be tiny: the antenna consists of a flat, metallic conductive coil rather than a protruding FM-style aerial (see figure 1), and the chip is potentially less than half a millimetre (Hitachi, 2006). These two components are usually attached to a flat plastic tag that can be fixed to a physical item. These tags can be quite small, thin and, increasingly, easily embedded within packaging, plastic cards, tickets, clothing labels, pallets and books. There are two main types of tags: passive and active. Passive tags are currently the most widely deployed as they are the cheapest to produce.

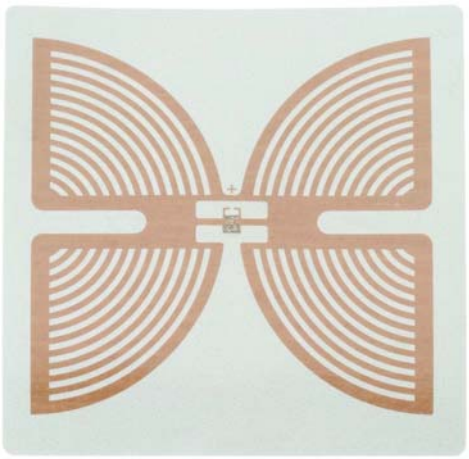

Figure 1: Class 1 tag insert (Butterfly style). Source: Courtesy of Intermec technologies

1.1.2 The Reader

The reader is a handheld or fixed unit that can interrogate nearby RFID tags and obtain their ID numbers using radio frequency (RF) communication (i.e. the process does not require contact). When a passive tag is within range of a reader, the tag's antenna absorbs the energy being emitted from the reader, directs the energy to 'fire up' the integrated circuit on the tag, which then uses the energy to beam back the ID number and any other associated information.

There are two main classes of RFID readers: read-only, an example being those that operate with the purely passive EPC Class 1 tags, and read/write, which can write new information back to a tag that has been equipped with a read/write memory. The readers are becoming increasingly sophisticated, acting as gateways into the network-centric communication systems of modern enterprises by supporting communication protocols such as TCP/IP and network technologies such as DHCP, UDP/IP and Ethernet or 802.11x (for wirelessly sending data back to the enterprise). Many models of reader are handheld devices and resemble the pricing guns or barcode scanners used in supermarkets, but readers can also be fixed in place (e.g. in doorways or at vehicle toll gateways) and even hidden, e.g. embedded into ceilings or walls.

There are also readers that can be incorporated into handheld devices such as PDAs and mobile phones (e.g. Nokia 5140, Nokia 3220 – see figure 2) and, in addition, class 5 tags are also known as 'reader' tags–devices that can read other RFID tags and exchange data with them.

Figure 2: Nokia 3220 phone. Source: Courtesy of Timo Arnall[1]

1.2 Why RFID is becoming important: Barcodes on steroids

RFID has a wide and growing range of potential uses throughout industry, commerce, education and the public sector more widely. The main driver for the development of the technology is the capability to identify and track the movement of products through the supply chains. This is important to retailers because it reduces the likelihood of items being out-of-stock, estimated, in retail, to have been around 4% of annual sales in 2003 (McFarlane, 2003) and reduces 'shrinkage' (loss of stock, including through theft) which is reported to have cost American companies $31.3 billion in 2003 (Deutsch, 2003).

The current method of product tracking within supply chains is the barcode, but passive RFID tags provide some simple, but fundamental, advantages. Firstly, barcodes are usually printed on paper labels or packaging, and are therefore prone to damage. Secondly, although barcodes can provide inventory data to the level of product category, they can not provide additional data such as 'sell by' dates[2]; this type of extra functionality has the potential to be developed further for things like home automation, where, for example, RFID tags embedded in clothes may, in the future, be able to provide washing instructions to washing machines. Also, because RFID systems use radio frequencies to communicate, they are able to identify an object without a line of sight. This means that RFID tags can be identified while they are attached to items inside boxes or pallets, or even behind walls. This results in increased automation of handling processes when compared to barcodes, as barcodes need a line of sight in order to work. It also provides the capability for multiple, almost concurrent reads (in actual fact these are consecutive, but very quick). This speed-up, when magnified throughout today's globalised supply systems, indicates the scale of efficiency that RFID could potentially deliver, and explains why a large

[1] http://www.elasticspace.com/

[2] the use of UCC/EAN-128 standards enable supplementary information such as "best before" dates to be added to the product code

number of corporate and global businesses have invested heavily in the development of these systems.

1.3 Why a TechWatch report

It is impossible to separate RFID technology from the concerns around its implementation, especially with respect to the potential for privacy infringement and identity theft. Although RFID implementation in the UK has been relatively uncontroversial so far, this does not mean that there are no issues that need to be addressed and a pro-active approach to the development of the technology, at this early stage, should be a priority for the F&HE community. This report therefore provides a brief discussion of some of these issues as well as a detailed examination of RFID technology, including some of the current uses within research, administration and teaching and learning. The report also includes an overview of the significance of RFID as an enabling technology towards achieving the 'seamless' and 'calm' vision of ubiquitous computing, the role of the Internet of Things, and plots a future trajectory for RFID development within the wider context of wireless, networked environments.

2. RFID TECHNOLOGY IN DETAIL

The radio frequency part of RFID is the communication medium between tags and readers. With passive RFID tags, radio frequency is also used to deliver power to the tag, as they do not have on-board power systems.

RFID systems are designed to be asymmetric: readers are expensive and power hungry, whilst tags are cheap and require comparatively low levels of energy. In addition, there are three key elements that need to be borne in mind in any discussion of RFID systems: energy source (which determines if a tag is passive or active), frequency and memory.

2.1 Energy Source: Passive or active?

RFID tags come in a variety of different types according to their functionality, and these types have been defined in an RFID Class Structure by the Auto-ID Center (and later through EPC Global) (Engels and Sarma, 2005), which has been subsequently refined and built on. The basic structure defines five classes in ascending order as follows:

Table 1: RFID class structure.

Class	*Class Layer Name*	*Functionality*
1	Identity Tags	Purely passive, identification tags
2	Higher Functionality Tags	Purely passive, identification + some additional functionality (e.g. read/write memory)
3	Semi-Passive Tags	Addition of on-board battery power
4	Active *'ad hoc'* Tags	Communication with other active tags
5	Reader Tags	Able to provide power for and communicate with other tags i.e. can act as a reader, transmitting and receiving radio waves

It is worth noting that the nomenclature for the classes has changed over time (RFID Journal, 2006) and older documents and specifications also refer to a Class 0 tag. This is a simple, passive tag which has had its ID programmed in *at the time of manufacture.* A Class 1 device (under this older scheme) is the same as a Class 0, but it can have its ID programmed into the tag at a later date, *after* manufacture. Both of these tags are read-only, in the sense that the ID can only be programmed in once. Later specifications work by EPC Global has clarified this by merging Class 0 and Class 1 into a new superseding Class 1 (Traub et al., 2005). However, there is still a considerable body of literature, specification documentation and manufacturer's material that refers to Class 0 tags and some tag manufacturers still offer a Class 0+ in which the ID is added at manufacture but can be altered later. For the purpose of this report we will consider Class 0 as absorbed into Class 1. It should be noted that Class 1 to 5 terminology is only used by EPC Global, and is not generic to RFID.

Each successive class builds on functionality provided by the lower layers and in order to understand how this works it is helpful to look at what is meant by passive,

semi-passive, and active. i.e. the use of harvested (or what is sometimes termed 'reflected') power and on-board power sources (Cheekiralla and Engels, 2005).

- *Passive Tag Systems* do not have an on-board power source so they have to 'scavenge' power from the reader in order to run the digital logic on the chip and issue a response to the reader. They can therefore only operate in the presence of a reader. The communication range is limited by the need for the reader to generate very strong signals to power the tag, which therefore limits the reader-to-tag range. In addition, the small amount of energy that the tag is able to harvest in order to power its response to the reader, means that the tag-to-reader range is also limited (to around four or five metres in UHF). However, as passive tags do not require a continuous power source they have a much longer lifecycle, and because of their minimal on-board circuitry they are much cheaper to produce. This means that passive RFID tags are more suitable for tagging individual product items for applications such as supermarket checkouts and smart cards.

- *Semi-passive Tag Systems* require the tag to use battery power for the digital logic on the chip, but still use harvested power for communication. Semi-passive tags are far more reliable and have greater read ranges than purely passive tags, but they also have shorter lives (due to their reliance on battery power), are more fragile, and are significantly more expensive.

- *Active Tag Systems* have an active radio frequency (RF) transmitter (i.e. they are capable of peer-to-peer communication) and the tags use batteries to power the logic chip and to communicate with the reader (i.e. they do not use harvested power). Read range increases (up to several kilometres) and reliability improves; active tags can be read while moving at up to 100 miles an hour (e.g. in automatic toll-road payment systems) and the readers are capable of reading up to a thousand tags per second. Active tags can also be equipped with built-in sensors e.g. for monitoring temperature control and reporting unacceptable fluctuations on refrigerated products whilst in transit, although this does increase the cost even more – to over £55 (around $100 or €80) per tag (IDTechEx, 2005). They also have a much larger memory than passive tags and, due to their higher processing capabilities, are also more secure.

2.2 Frequency

RFID is fundamentally based on wireless communication, making use of radio waves, which form part of the electromagnetic spectrum (i.e. frequencies from 300kHz to 3 GHz). It is not unlike two other wireless technologies, WiFi and Bluetooth. The three technologies are all designed for very different uses and therefore have different functionalities but there is shared ground between the three, with some hybrids starting to appear. RFID systems can utilise both WiFi and Bluetooth and need not see them as competitors.

RFID operates in unlicensed spectrum space, sometimes referred to as ISM (Industrial, Scientific and Medical) but the exact frequencies that constitute ISM may

vary depending on the regulations in different countries[3]. These operating frequencies are generally considered to be organized into four main frequency bands and the table shows these different radio wave bands and the more common frequencies used for RFID systems (IEE, 2005).

Table 2: RFID operating frequencies and associated characteristics.

Band	**LF Low frequency**	**HF High frequency**	**UHF Ultra high frequency**	**Microwave**
Frequency	30–300kHz	3–30MHz	300 MHz–3GHz	2–30 GHz
Typical RFID Frequencies	125–134 kHz	13.56 MHz	433 MHz or 865 – 956MHz 2.45 GHz	2.45 GHz
Approximate read range	less than 0.5 metre	Up to 1.5 metres	433 MHz = up to 100 metres 865-956 MHz = 0.5 to 5 metres	Up to 10m
Typical data transfer rate	less than 1 kilobit per second (kbit/s)	Approximately 25 kbit/s	433–956 = 30 kbit/s 2.45 =100 kbit/s	Up to 100 kbit/s
Characteristics	Short-range, low data transfer rate, penetrates water but not metal.	Higher ranges, reasonable data rate (similar to GSM phone), penetrates water but not metal.	Long ranges, high data transfer rate, concurrent read of <100 items, cannot penetrate water or metals	Long range, high data transfer rate, cannot penetrate water or metal
Typical use	Animal ID Car immobiliser	Smart Labels Contact-less travel cards Access & Security	Specialist animal tracking Logistics	Moving vehicle toll

N.B. Within a given frequency band the actual, real-world communication range will vary widely depending on factors such as the operating environment, the detail of the antenna design and the available system power (Dressen, 2004; Paret, 2005).

[3] Due to the value of communication in the EM spectrum, most of it is controlled by both national and international regulation. In Europe, RFID is the driver behind a re-think of EM spectrum regulation (European Commission, 2006) but it seems unlikely in the current climate that this will be replicated at a global level. It is therefore important that RFID systems and applications allow for multiple frequency tags and readers.

There are two types of RFID system, each using different physical properties to enable communication between the reader and the tag (Thompson, 2006). The physics employed can become complex, but it is important to realize that it partly determines the operating range of the systems. RFID systems based on LF and HF frequencies make use of **near field** communication and the physical property of *inductive coupling* from a magnetic field. The reader creates a magnetic field between the reader and the tag and this induces an electric current in the tag's antenna, which is used to power the integrated circuit and obtain the ID. The ID is communicated back to the reader by varying the load on the antenna's coil which changes the current drawn on the reader's communication coil; further detail of the physics of the operation can be found in ACM Queue's RFID special edition (Want, 2004). RFID systems based on UHF and higher frequencies use **far field** communication and the physical property of *backscattering* or 'reflected' power. Far field communication is based on electric radio waves: the reader sends a continuous base signal frequency that is reflected back by the tag's antenna. During the process, the tag encodes the signal to be reflected with the information from the tag (the ID) using a technique called modulation (i.e. shifting the amplitude or phase of the waves returned).

2.3 Memory

Tags come in a variety of forms with varying types of on-chip memory capability. Tags can be read-only (the unique ID code is permanently stored on the tag – also known as WORM: Write Once Read Many), read/write (allowing a user to change the ID and add additional data to the tag's memory), or they can be a combination, with a permanent tag ID and some storage space for the user's data.

Passive tags typically have anywhere from 64 bits to 1 kilobyte of non-volatile memory. Active tags tend to have larger memories with a range of, typically, between 16 bytes and 128 kilobytes (Dressen, 2004; Zebra website[4]).

2.4 Standards

The number and use of standards within RFID and its associated industries is quite complex, involves a number of bodies and is in a process of development[5]. Standards have been produced to cover four key areas of RFID application and use: air interface standards[6] (for basic tag-to-reader data communication), data content and encoding (numbering schemes), conformance (testing of RFID systems) and interoperability between applications and RFID systems (RFID Journal, 2006).

There are several standards bodies involved in the development and definition of RFID technologies including:

- International Organisation of Standardisation (ISO)

[4] http://www.zebra.com/id/zebra/na/en/index/rfid/faqs/rfid_tag_characteristics.html
[5] A more detailed explanation of standards can be found at RFID Journal's website (www.rfidjournal.com)
[6] Air interface standards cover the Physical and Data Link layers of the basic OSI communications model (i.e. the lowest layers of a communications protocol)

- EPCglobal Inc™[7]
- European Telecommunications Standards Institute (ETSI)
- Federal Communications Commission (FCC)

2.4.1 Air interface (frequency) standards

RFID frequencies (as outlined in table 2) are governed by the ISO 18000–RFID Air Interface family of standards, and a complete set of standards was released in September 2004:

ISO 18000-1 – Generic Parameters for the Air Interface for Globally Accepted Frequencies
ISO 18000-2 – for frequencies below 135 kHz
ISO 18000-3 – for 13.56 MHz
ISO 18000-4 – for 2.45 GHz
ISO 18000-6 – for 860 to 960 MHz
ISO 18000-7 – for 433 MHz

There are also earlier standards relating to, for example, cattle tracking systems (ISO 11785), tag-based payment "proximity" cards (ISO 14443) and electronic toll collection "vicinity" cards (ISO 15693). ISO 14443 and ISO 15693 both operate at 13.56MHz (HF), but the first standard has a read range of about 10cm whereas the later has a read range of 1 to 1.5 metres.

The situation regarding frequencies is somewhat confused by the introduction, by EPC Global, of a separate air interface standard for UHF frequencies (covered by ISO 18000-6) for their early class 0 and class 1 tags. These tags are not interoperable with each other, nor are they compatible with ISO's air interface standards (RFID Journal, 2006). EPC Global has subsequently developed a second generation of protocols (GEN 2) that merge the old Class 0 and Class 1 passive tags and should be more closely aligned with the ISO, although disagreements remain between the two organisations at the time of writing. Obviously, supply chain managers and equipment vendors would like to see an agreed, international standard.

2.4.2 Data content and encoding

As supply chains involve moving goods between large numbers of disparate organisations and locations, there is a requirement for all parties involved to use a standardised form for the identification of products. The Auto-ID Center at MIT was responsible for much of the development of recent RFID technology and standards work, particularly around supply chain management. Some of this work has now been transferred to the EPC Global[8] organisation (as the Auto-ID Center closed in October 2003, although some of the more research-based work is continued through a network of Auto-ID labs in universities across the world[9]).

EPC Global has defined standards for a range of features of global RFID systems

[7] EPCglobal describes itself as a neutral, consensus-based, not-for-profit standards organisation which is owned jointly by GS1 and GS1 USA (two members-based organisations for the supply chain industry)
[8] http://www.epcglobalinc.org/
[9] http://www.autoidlabs.org/

including unique identification system protocols (the Electronic Product Code, or EPC™) for tag to reader communication, specification of middleware systems to handle EPC codes, a mark-up language (Physical Mark Up Language) and the Object Naming Service (ONS)[10]. These are described in detail below:

2.4.2.1 Electronic Product Code

A crucial component in the development of RFID was the introduction of the Electronic Product Code (EPC™). In short, this is the unique code number that is embedded into the RFID tag's memory. It is a generic, universal numbering scheme for physical objects, similar in scope to the barcode numbering scheme (UPC). However, there is one fundamental difference between the EPC and the UPC: the EPC has the capability to identify every single, individual product item. Whereas the barcode on a tin of baked beans will provide a codification for the manufacturer and the product (e.g. a 12 oz tin of beans), it does not provide for identifying a *particular* tin of beans. The Auto-ID Center's numbering system provides much greater scope for identification than barcodes, and consists of a 96-bit number, structured as follows:

01.	0000A89.	00016F.	000247DC0
Header	EPC Manager	Object Class	Serial Number
8 bits	28 bits	24 bits	36 bits

It is in fact not a single numbering system, but a "federation" of several naming structures (Traub et al., 2005). The Header bits define which of several coding schemes is in operation with the remaining bits providing the actual product code. The scheme is designed, in part, to accommodate existing global numbering systems such as the Global Trade Identification Number (GTIN), Serial Shipping Container Code (SSCC), and the Global Location Number (GLN). The Manager number identifies the company involved in the production of the item (manufacturer) and the object class defines the product itself. The Serial number is unique (within the scope of the other numbers) for an individual product entity. The 96-bit code can thus provide unique identifiers for 268 million companies (2^{28}). Each manufacturer can have 16 million (2^{24}) object classes and 68 billion serial numbers (2^{36}) in each class (Moroz, 2004).

2.4.2.2 Alternatives to EPC: IPv6

Some researchers believe that the architecture of the Internet offers a clear series of principles for developing the new communication capability for individual physical items and devices.

IPv6 is a network layer standard that governs the addressing and routing of data packets through a network. It is a numbering scheme large enough to give 430 quintillion addresses for every square inch of the world's surface, in comparison to IPv4 (the current system), which has the capacity to support 4 billion addresses[11].

[10] http://www.nje.ca/Index_RFIDStandards.htm

[11] http://en.wikipedia.org/wiki/Ipv6 [last accessed 10/04/06].

It has been suggested that IPv6 could be used in conjunction with RFID, leaving the EPC™ redundant, and the US Department of Defense has already mandated that its battlefield network should use IPv6 by the end of 2006 (RFID Journal, 2003). However, Daniel Engels of the Auto-ID Center (2002) believes that 'the requirement to interpret an IPv6 identifier as an address for IP communication prevents its use as a permanently assigned identifier on mobile objects' (p. 6). In addition, due to the development of standards and the fragmentation of the RFID market (in terms of both technologies and applications) it is unlikely that IPv6 currently holds a direct threat to the adoption of the EPC™.

2.4.3 ISO Testing and Conformance

Standards for testing the conformance of RFID equipment to the operating standards and for measuring the performance of equipment are covered by ISO 18047 and ISO 18046 respectively.

2.4.4 Interoperability between applications and RFID systems

The EPC Network Architecture

RFID tags and interrogators are rarely used in isolation; they form part of a supply chain, or a logistics, library or other system. The key concept is that the ID code embedded on an RFID tag can provide what database designers call a 'primary key' into a database of products. All additional data associated with that item can be stored in back-office databases and systems. The Auto-ID Center has developed an architectural overview and vision for the use of the EPC™ unique identifier in supply chain systems, known as the EPC Network Architecture. The architecture is layered, with tags and their associated readers operating at the bottom of an integrated system that is linked to database and manufacturers' back-office enterprise systems.

The exact operational details of this complex architecture are beyond the scope of this report, however, we will note of some key components and related standards. Those interested in a more detailed examination of the network architecture, see Synthesis, 2004.

Savant

Savant is the middleware software system that links reader devices and processes the information streams from tags. It acts as the gateway to the enterprise systems and database applications, providing filtering, aggregation and counting of tag-based data.

ONS

The Object Naming Service (ONS) is 'the 'glue' that links the EPC™ with the associated data file' (Brock, 2001, p.1). Working much like the current Domain Naming Service of the World Wide Web it provides a look-up table for translating a unique EPC code into a Uniform Reference Locator (potentially a webpage) where additional information can be stored. The ONS system is built on the same technology used in the Internet's Domain Name Service (DNS) (Brock, 2001).

Physical Mark Up Language

The Physical Markup Language (PML) is an XML-based common language designed to provide standardised vocabularies for describing a) physical objects, b) observations made by sensors and RFID readers about these objects and c) the observers (the sensors and readers) themselves and exchanging this data between entities operating within the EPC™ network architecture. PML uses the W3C XML Schema language (XSD) for its definition. Full details can be found in (Floerkemeier et al., 2003).

The difficulty in describing physical objects is acknowledged by the Auto-ID Center (Brock et al., 2001), but the intention of PML is to give a structure to agreed object characteristics such as volume, mass, temperature, owner, location etc.

3. RFID APPLICATIONS IN EDUCATION

It is clear that the majority of envisaged commercial applications for RFID revolve around improving the supply chain, stock control and logistics and that as consuming entities universities and colleges will increasingly be handling and working with physical equipment and resources that involve RFID labelling and tagging (for example, expensive medical equipment is beginning to be tagged in large hospitals to allow tracking and prevent loss). It should be noted that, although it is beyond the scope of this report, there are health and safety implications for workers using RFID equipment, especially those with active, implanted medical devices such as cardiac pacemakers (HSE, 2003). The EU Directive 2004/40/EC (due to be implemented from 2008) sets out to provide a minimum level of protection for workers, but its scope is limited (in terms of the health issues it covers) and its focus has changed since its original inception. These issues are complex and work is ongoing; interested readers should investigate the work of the Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR)[12] and EMF-NET[13], the EU's Co-ordination Action that aims to provide a framework for the co-ordination of the results of the research activities related to the biological effects of electromagnetic fields, including occupational exposure.

3.1 RFID in Libraries

For many years, libraries have used a combination of technologies to reduce the likelihood of theft, improve stocktaking, and speed up issue and return procedures. The advantage of using RFID is that it is capable of incorporating and improving upon existing systems within one technology. For example an RFID reader does not need a direct line of sight, which means that books do not have to be tipped out or even pulled out completely as with barcode scanners, so inventory checking is faster and can be done more frequently. Also, RFID tags do not need to be read individually as barcodes do as RFID scanners can read stacks of books at a time, saving time, and potentially reducing health problems caused by RSI. Other benefits of RFID include simplified and faster issuing of books, self-return (the ‘ATM approach’ to returning books), and rapid location checking of books (Gilbert, 2004b).

There are two main types of system that can be used in libraries, both of which involve each book being tagged with an RFID chip which either contains bibliographic data (bibliographic method) or a simple reference to detailed bibliographic information held off-chip in the library databases ('name plate' or 'licence plate' systems). At the moment, the bibliographic system is not used very much in the UK, although there are discussions taking place around possible data objects for encoding selected bibliographic data within library tags (Praxis, 2006). These systems allow a self-checkout process when books are borrowed: as the books pass a special RFID reader at the check-out desk the tag is scanned and the item is recorded as borrowed by the identified student or staff member. Apart from being faster, this system also frees up library and information staff from carrying out more mundane checkout tasks.

[12] http://europa.eu.int/comm/health/ph_risk/committees/04_scenihr/docs/scenihr_q_005.pdf
[13] http://www.jrc.cec.eu.int/emf-net/index.cfm

So libraries have become early adopters of RFID, and in the US more than 300 public and college libraries have adopted RFID (Gilbert, 2004b). In fact, library implementations are important test-beds for the technology. They have discovered that the 'tuning' of the RFID interrogator's detection field can be critical in a system's security as leaving tagged items in close proximity to an issue/return station can result in them being discharged or issued unintentionally; in some instances, incorrect tuning of the detection field also meant that it was possible to evade the field completely (Marsterson, 2006).

There is also a strong economic argument in favour of tagging valuable items such as library books. To date, uptake of RFID in general has been limited because even passive tags are still relatively expensive to produce (around 27 pence or 50 American cents, although this is continually reducing), so it makes no economic sense to tag inexpensive items (such as individual tins of baked beans). Within libraries, where individual books and journals can be worth hundreds of pounds, and will be borrowed and returned hundreds of time, the one-off cost of a tag is more than off-set by cost savings and efficiency gains.

In the UK, Glasgow University Library was the first university library to install RFID (in 2002) and has been joined subsequently by a small number of university libraries including Middlesex and Nottingham Trent University. Similar systems are also being introduced in public libraries such as Norwich, Essex, Haringey, Somerset and Sutton, and CILIP – the library professionals association - recently held their first major conference on the subject and have subsequently produced an RFID implementation checklist[14]. Standardisation work has also been strong in the library sector: in the UK the BIC/CILIP RFID in Libraries Committee has been working on possible data objects for library RFID systems and in Denmark, the national library authority developed a Working Group to bring together interested parties in the development of an RFID data model for libraries that has fed into the ISO TC46/sc4 work on the standardisation of protocols, schemas and related models and metadata.

This position as early adopters, who also have a considerable amount of group bargaining power and a strong interest in developing standards, puts libraries in an interesting position. It could be argued that libraries are uniquely placed to have a positive impact on the development of RFID technology and that this influence could extend beyond current efforts to develop interoperability and data standards, to addressing more general issues that are 'in the public good' such as privacy concerns (see section four). Issues such as whether or not RFID tags are implemented in students' library cards and the frequencies that RFID interrogators operate at (i.e. open or regulated) are simple, but important starting points. It should also be noted that Danish libraries are generally accepted to be at the forefront of library-based RFID development, and that JISC's collaboration with the Danish National Library Authority along with the recent instigation of the Knowledge Exchange provide a timely opportunity for international collaboration and good practice sharing.

[14] Available from BIC (Book Industry Communication) by e-mail: rfid (at) bic.org.uk.

3.2 Asset Location Management

Hospitals around the world are starting to use RFID tags to track and manage assets, particularly expensive or critical items of equipment such as ventilators, electrocardiogram devices and infusion pumps. These systems, known as Real Time Location Systems or Enterprise Asset Visibility systems, tag physical items of equipment and make them 'visible' to hospital managers via the hospital's WiFi network. This means that hospital staff can always locate valuable or important equipment very quickly, which increases efficiency (one hospital in America estimates savings of nearly 8,000 minutes per month) and can even save lives (Wexler, 2005). Such systems may well be introduced into UK university medical schools and the same technology could be used for tracking highly mobile equipment (such as laptops, projectors, research monitoring equipment etc.) within UK academic environments.

The use of RFID technology is also starting to have implications for document tracking and business process workflows, an important issue in college and university administration departments and for registrar activities (e.g. tracking of completed exam papers). RFID tags in the form of labels that can be written on can be attached to paper documents. The tag's unique ID can be scanned by readers as the document passes through the administration system. By referring the tag ID back to a database of other information such as the document's history and expiration date, the document's status can be tracked. As readers can then obtain information from the label without line of sight scanning it would be easy to locate a mis-placed document simply by scanning a shelf of papers and books, and this would be particularly useful for university paper archiving systems.

3.3 People tracking and tagging

There could be a number of applications for RFID within education related to security and the identification of staff and students, but this, of course, is controversial as there are serious concerns over privacy. RFID technology can be used for the identification and location tracking of a person carrying the tag (which can be embedded into an identification card) and can be used to verify a person's right to enter a particular building or even to access a service. For example, in the US, RFID-enabled cards are used to automatically register students at lectures, and in China, nearly 3,000 universities have installed RFID tag readers, for use with RFID-enabled student identification cards, contactless library applications, and to reduce train travel fraud (Collins, 2003).

Subcutaneous RFID tags, about the size of a grain of rice, have also been approved for use by the US Food and Drug Administration (Gilbert, 2004a). The tags are injected into the fatty tissue of the arm and provide an ID that can be linked to a patient's hospital records.

3.4 Intelligent Buildings and disabled access

RFID tags are being increasingly used as one tool in the development of a more user-focused experience for visitors to museums, galleries and similar spaces. For example, at the Exploratorium, a science museum in San Francisco, visitors wear an

RFID-enabled card through which they interact with networked RFID readers, which are mounted on museum exhibits. The exhibits are hands-on experiments which visitors take part in (for example, a heat camera that shows a thermal image of the body). As the visitor takes part in an exhibit experiment their RFID tag is read and this triggers a camera to record the experiment. The results of these experiments are automatically uploaded to a personalised webpage for the visitor, which provides a record of their visit (His and Fait, 2005). Museums and galleries have also used RFID tracking when moving art works and other expensive pieces (Katz, 2005).

Researchers at the University of Florida are developing a system to help blind students make their way around campus. The Drishti project makes use of various technologies including an information 'grid' based on passive, low-cost, high frequency RFID tags installed under the flooring which is used to convey precise location and detailed attributes about the surrounding areas. RFID tags are placed along corridors, inside rooms and even outside, and store information about their immediate surroundings. An RFID reader is incorporated into a walking cane and shoe and uses sound to deliver directions (Willis and Helal, 2005).

3.5 Research applications – Equipment and Activities

Research Equipment

Products are becoming available that incorporate RFID into laboratory equipment for research and medical work. The use of RFID tagging on, for example, test tubes, is designed to reduce human error. In addition, processes are much faster because RFID tags can be read in large quantities and data can be synchronised with client databases.

Research activities

RFID tagging is being increasingly used as a research tool in experiments and investigations. This is particularly true in biology and ecological studies where tagging of wildlife and monitoring of feeding and migration has been carried out for some years using forms of remotely monitored tag[15]. One example of this type of use is Digital Angel's RFID system in Colombia, Ohio (USA) to monitor the movement of salmon within the river system and at dams[16].

In addition, RFID tags with in-built temperature monitoring systems have recently been proposed for monitoring the health of large numbers of farm poultry with a view to early detection of avian flu symptoms (Using RFID, 2005). A handheld RFID reader can take in the ID and temperature of large numbers of birds at a very fast rate.

A number of research projects are also being undertaken within computer science and healthcare that explore the activities of daily living in order to infer information about daily human activity through monitoring the objects that people make contact with and handle. Within community medicine this enables homes to be more 'helpful' to individuals by, for example, providing enhanced facilities for the elderly that allow them to remain in their own homes (Philipose et al., 2004).

[15] http://www.biomark.com/
[16] http://www.digitalangelcorp.com/about_pressreleases.asp?RELEASE_ID=211

3.6 RFID in new Learning Environments

RFID tags are an increasingly important component in the toolkits that are being developed for exploring new learning environments through the use of gaming, location-based services, tangible interfaces and augmented reality (see Benford (2005) and O'Malley and Stanton (2005) for a general overview, and the NESTA Teaching with Games project http://www.futurelab.org.uk/research/teachingwithgames.htm for specific insight into the ways in which commercial games might be implemented in a formal educational setting). In these types of contexts, children or students enter the RFID-enabled environment with RFID reader devices and interrogate RFID-enabled 'objects' (physical entities in the environment such as toys, the flash cards used in games etc.) in order to control the flow of events and initiate their own access to information. In this way, RFID tags are used as a way of embedding user control within learning and gaming environments.

Although to date these environments have been explored in the context of younger, school-aged children it is likely that more sophisticated versions of such environments will be introduced into Higher and Further education in coming years. These new learning environments are providing important test-beds for developing these ideas within an educational context.

4. SOCIO-CULTURAL IMPLICATIONS

4.1 RFID and privacy

The introduction of RFID tags, particularly into the consumer supply chain, has not been without controversy, although the US has borne the brunt of this so far. There has been considerable concern about the implications for individual privacy, especially with the recent publication, by the IEEE, of a paper concerning RFID viruses (Rieback et al., 2006). As it is likely that HE and FE will increasingly be using RFID in libraries, administration and research it is worth being aware of the nature of the controversy and some of the implications.

Most of the concerns stem from the fact that once individuals move around in a world of widespread tagging, the products they buy, wear and consume will be capable of being identified and recorded by a widespread network of readers. Such information could provide a great deal of intelligence on a person, their habits, likes and dislikes and movements. In essence this is an aspect of a person's individuality and the right to privacy should be paramount. The argument is that by mining the data about the position and movement of 'things' one can obtain information about people, forming knowledge from 'the collection of diverse data from everyday life' (Hennig et al., 2004, page 5).

In the case of passive tags, a signal from an RFID reader causes the tag to beam back its unique ID along with any other information it has been programmed to relay. In this scenario there are two types of potential privacy infringements that could take place. Firstly, bearing in mind that the transponder and interrogator are connected to an 'intelligent' back-end system that stores information related to the unique ID, there is the potential for privacy infringement or identity theft either through poor information management, poor system security, or virus attack. The second type of infringement is related to the nature of the 'other information' that is programmed into the tag. As an example, the use of bibliographic tags within library RFID systems, whilst useful to libraries because they help to alleviate potential vendor lock-in and facilitate services such as inter-library loans, have been the subject of concern by privacy activists since by programming bibliographic information onto the tag, there is the potential for a privacy infringement from non-library interrogators. Bearing in mind that RFID readers are now starting to appear in mobile phones, it is possible for a borrower's books to be interrogated whilst still in their bag or rucksack (although the interrogator would have to be very close – say on a crowded tube train). The owner of the RFID interrogator would then be privy to information about the library user's reading habits, which, in itself, would be a breach of the library user's privacy. However, the concern is that information gleaned from this type of privacy attack may then be used more widely for impersonation or identity theft.

4.1.1 RFID and the surveillance society

Within consumer scenarios, concerns have been raised about the capability to use RFID to track a customer's movement around a shop. This concept is not a new one for consumers, as most people are familiar with CCTV tracking, but RFID tracking logs are significantly smaller than CCTV output and are machine-processable

(Engberg et al., 2004). To some people this may in itself be considered an invasion of privacy, but additional problems occur when shops keep persistent records that are traceable to identifiable customers. This problem is compounded when, for example, the RFID tag's unique ID can be obtained by any reader and that reader can also connect to the back-end RFID infrastructure (either through legal or illegal means), linking the unique ID to detailed tag information and even the purchase transaction.

Some authors have argued that these problems are issues of RFID system security: if RFID systems were better designed, and had security at the heart of the design, then these kinds of privacy invasion would not be possible (Engberg et al., 2004). However, this assumes that there is a sufficiently robust legal system in place to redress the issue of people or organisations that do not deploy these 'secure' tags, and further, that the victim of the privacy invasion or identity theft is aware of when an 'illegal' RFID-enabled transaction is taking place. This means that ordinary consumers would need to be aware of issues such as when data collection is taking place, the potential use this data may be put to, and the potential consequences of both of these.

An example used by anti-RFID campaigners provides a case in point for some of these issues. In Germany, the METRO Extra Future Store was set up as a test-bed for new 'intelligent' technologies, including a small selection of RFID-tagged items (Weber, 2004). Without going into a detailed description of what the campaigners found[17] it appears that there were significant breaches of policy, resulting in 'hidden' tagging of customers through the shop's loyalty card. In addition, the shop's deactivation technology, designed to disable the passive RFID tags attached to individual items, was not completely successful, leading to some tags remaining 'live' even after customers had left the shop. Activists point to a scenario where a passive RFID tag, embedded in a new shoe, could be providing information to tag readers wherever the person walks: this information could then be combined to form a picture of a person’s movements.

These examples demonstrate several factors that can be extrapolated to give a more conceptual picture of the potential for privacy invasion: the ubiquity of RFID readers and tags and the fact that they can be hidden; the linking of a unique ID to other information contained in a database or other storage system; security and privacy risks that are created either maliciously or through neglect.

4.2 Approaches to Privacy Protection

In a consumer scenario the most obvious solution to the RFID privacy problem is to disable the tag at the point of sale. However, this is meaningless if the deactivation system is not completely reliable. Also, while it may be appropriate to disable some tags at the point of sale, other tags, e.g. passive tags in library books or active tags used in road toll systems have to remain 'live' while in the possession of the customer.

Disabling RFID tags in consumer environments at the point of sale also means that the tag cannot be used by consumers as an enabling technology for ambient intelligence applications, for example, in advanced recycling applications where the

[17] more information can be obtained from the Spychips website: http://www.spychips.com/metro/scandal-payback.html

tag's unique ID could be used to automatically sort recyclable material and could also be used to levy waste charges on the manufacturer based on the nature and volume of rubbish collected. Passive RFID tags used in consumer environments could also be used to deliver after sales services for product service records or to provide warranties.

In order to try to address these issues there have been proposals for 'secure' tags equipped with 'handover protocols' to facilitate the transfer of ownership of the unique ID (so that different sets of readers would be able to read the tag at certain points in time) and systems that support 'multiple authorisations', where readers belonging to several authorised 'actors' may be able to read the tag at the same point in time (e.g. the consumer and the after sales service provider may both access the tag while the product is under warranty). However, it should be noted that solutions based on consumer consent offer no guarantee of privacy protection and may turn into some sort of advanced blackmail, where consumers have the impossible choice of not getting a service (e.g. warranty protection) unless they agree to the collection of personally identifiable information (Engberg et al., 2004). In addition, these types of advanced systems assume that the owner is capable of managing the technology and actually 'trusts' it to work as described.

4.3 Trusted computing, beta culture and the DIY culture

In order for RFID to be widely adopted it needs to be accepted as credible and trustworthy. This is an area of computing that is growing in importance, especially in a world where the speed of technological innovation and route to market of new technology products is challenging the historical view of computers as being highly credible (Fogg, 2003). Part of the reason why RFID is perceived as not being trustworthy is due to a lack of belief, on the part of the consumer, in their ability to have any control over the technology. Whatever the truth may be about the actual control they can exercise over the technology, their perception is that they in fact have very little control, and that is why it is not seen as either credible or trustworthy.

Other developments, such as releasing software products 'in beta' are also acting to further undermine the trustworthiness of computers. This is often regarded as a 'new model for how software companies can get new products or features out into the marketplace quickly, then improve them as they're used' (Carr, 2006) but it is also (cynically) seen as a way of potentially avoiding lawsuits or as a lazy approach to product development.

As a response to this, increasing numbers of technology consumers who have grown up with digital technologies and who are not afraid of taking them apart are modifying or 'modding' them to their own requirements. Web-based magazines such as Makezine.com and Zapped! (www.zapped-it.net) explain how to create RFID-enabled front doors and RFID blockers, and report on keyring devices for detecting nearby RFID readers. In addition, sites such as RFDump (www.rf-dump.org) have developed tools designed to demonstrate the vulnerability of RFID readers and the data they process, whilst in Korea, people have been melting the plastic cover of smart cards in order to retrieve the RFID chip inside in order to incorporate it into their portable gadgets or handbags (Jin-seo, 2005). It is important to note that many of these activities stem from the view of RFID as a 'participatory' technology and that in

the future this 'can do' group of technologically savvy people may be able to address their privacy concerns directly by taking matters into their own hands.

4.4 Privacy legislation and regulation

These issues have not gone unnoticed. In 2004 the National Consumer Council held a summit in the UK driven by the feeling that 'this technology is being developed and implemented without the knowledge or participation of consumers more widely' (Lace, 2004, p. 1). There were a number of recommendations from the summit, including:

- Review data protection laws and regulations
- Fund further research into consumer's perceptions of RFID technology
- Improve dialogue with consumers over the benefits and risks of RFID
- Explore these issues in the wider context of the information society and the increasing amount of data gathered on individual consumer's behaviour
- Build privacy protection into the technology

Similarly, in the US, the National Research Council's Committee on Radio Identification Frequencies Technologies held a workshop that observed that:

> 'on the consumer and regulatory side, there are many concerns and unanswered questions about the technology—for example, what are the ramifications for personal privacy of embedding RFID tags in consumer products? Indeed, more than one company has had to change or rethink its plans for RFID technology because of the concerns of consumers and privacy advocates about how the technology would be used.'
>
> (NAP, 2004, page vii).

Closer to home, the European Commission has just launched a public consultation on RFID, following on from the RFID inter-service group established last year to co-ordinate the gathering, analysis and internal dissemination of information concerning RFID technology and its uses. Outputs from the public consultation will be published as an online consultation document in September 2006 before the preparation of a Commission Communication on RFID, which is expected to be adopted before the end of the year. The Communication will also address the need for other legislative measures for RFID, such as decisions on allocation of spectrum and could lead to amendments of the e-privacy-Directive, which is up for review (European Commission, 2006).

The Commission is also planning to support, in the forthcoming Seventh Framework Programme for Research and Technological Development, technology and innovative applications that bring us a step closer to the 'Ambient Intelligent Society'.

There is no doubt that there are serious issues that will have to be dealt with seriously. Technologists, proponents of RFID and privacy experts are beginning to debate and address the issues raised by consumer groups, civil liberties groups etc. The issues that are engaging these groups include debating what privacy means in a technologically rich world, developing models of privacy threat, how to determine

whether a proposed technology can be adjusted in order to meet concerns and detailed technical solutions to situations.

5. THE IMMEDIATE FUTURE: THE FIVE-CENT TAG

The potential of RFID ubiquity through item level tagging has hinged around some technical and economic challenges. For global RFID adoption, systems will have to be interoperable (therefore reliant on protocol standards) and economically viable. In 1995 Noel Eberhardt (Motorola) and Neil Gershenfeld (MIT Media Lab) started collaborating in order to achieve a cost effective design for an RF tag, where the goal was to design the 'penny tag' (i.e. one American cent) (Schmidt, 2001). Eleven years later the industry is still struggling with the technical challenges this problem presents. In recent years, the goal has been set a little lower – the hunt for the 5¢ tag is on.

Whenever the 5¢ tag is achieved, it is important to understand the most likely characteristics and functionalities of the tag. In short, the tag will need to be passive (manufacturing and component costs means active and semi-passive tags are unviable), with low memory (in the region of 64 bits - smaller memory means less silicon and therefore lower costs) and no re-write functionality.

6. THE FUTURE AND THE BIGGER PICTURE: TOWARDS AN INTERNET OF THINGS

> *"Conceptualizing them simply as ID tags greatly underestimates their capabilities, considering some have local computing power, persistent storage, and communication capabilities"*
>
> Vince Stanford, 2003, p. 9.

RFID systems are part of a bigger picture and are potentially a key stepping-stone in the development towards the vision of ubiquitous computing. In the ubiquitous (ubicomp) or pervasive computer vision there will be a multitude of computationally capable, small - sometimes invisible to the human eye - devices that will be scattered throughout our environments, operating silently and largely unseen as they go about their individual tasks to support our daily activities. This will be a device-centric future with highly distributed network control.

In a step-change that will be orders of magnitude greater when compared to today's computing power, a bewildering population of heterogeneous sensors, computers and actuators will be operating. Often, these devices will operate with self-awareness (being 'conscious' for example, of their physical location and their immediate surroundings) and be widely networked together. In order to realise this vision a comprehensive jigsaw of technological 'pieces' needs to come together and converge as technology develops over the next few years. The RFID piece of the jigsaw is the ability for individual (physical) items to be able to identify themselves to the network.

A key concept in this development trajectory is the **Internet of Things**. A term first coined by RFID developers in the Auto-ID Center in the late 1990s, it is also sometimes referred to as the Product Internet, T2T (Thing to Thing) network, or the M2M (Machine to Machine) network. In this vision, increasingly large numbers of our everyday objects and gadgets will have some kind of simple communication technology embedded into them, allowing them to be connected to each other within local networks and, ultimately, connected to the wider network of networks – the Internet. In a sense this is a process of extending the Internet beyond computational devices down to a lower layer in the hierarchy of machines – to that of simpler devices and individual items (Krikorian and Gershenfeld, 2004). In order to facilitate this process, three areas need to be developed. Firstly, each of these items must be able to *identify* itself to other items and to the network in general. This is provided for by the introduction and development of RFID technology. Secondly, these items should include some element of embedded computational power in order to act with some level of 'intelligence'. Thirdly, they will need to have some sense of their physical environment and geographical location. Continuing developments in computational science and electronics, particularly work on miniaturisation, tiny operating systems and wireless communication will make this vision increasingly realistic (International Telecommunication Union, 2005). The basic RFID system of transponder and interrogator is an important starting point in the process.

6.1 From identification to Wireless Sensor Networks

At the lower (passive) end of RFID technology the systems simply provide a tag that can remotely identify an object by returning an ID when interrogated over short ranges. As RFID systems are introduced and find acceptance in business and other environments the functionality provided by these low cost tags will be increasingly seen as insufficient as new applications are developed (Engels and Sarma, 2005). There is likely to be a natural progression for RFID that includes the widespread incorporation of sensor functionality (Jarosik, 2005). Such devices will be able to make measurements concerning their surroundings and physical location about such variables as pressure, temperature, flow rate, speed, vibrations etc. (Allan, 2005). They will be networked either through RF technologies or through other wireless communications systems and these developments are often referred to as sensor nets, integrated on-chip radios, or wireless networked sensors (WNS). These types of networked, RFID-enabled objects will become similar to what Bruce Sterling (2004) calls 'spimes'. They will have histories (e.g. every time they are accessed they will record the details of that access), they will be 'precisely located in space and time' and they will become 'protagonists of a documented process' (Sterling, 2004).

These RFID-based sensors will need to communicate in order to participate in the network of things. However, other computational devices within the likely ubicomp jigsaw will not necessarily be using radio frequency for communication. Other protocols currently proposed or developed include ZigBee, Near Field Communication Technologies (NFC), Bluetooth and Wifi – all systems that offer local and personal area networks (LANs and PANs).

Zigbee is focused on individual devices (such as smoke alarms, lamps and consumer electronics) that need a robust, low bandwidth, low cost, low power, peer-to-peer communication. NFC is designed for very short-range communication (devices have to almost touch for the signalling systems to work). The applications being developed for NFC to date revolve around situations where it is intuitive for devices to touch in order to communicate e.g. allowing mobile phones to act as electronic tickets or electronic cash wallets when pressed against a suitable reader or kiosk device.

Some commentators see these developments as tending towards a form of ubiquitous wireless communications network which encompasses low-bandwidth systems such as RFID, computational and peripheral device networking through ZigBee, NFC and Bluetooth (e.g. digital cameras and printers), and higher bandwidth (telecommunication) devices through 4G cellular and WiMax (Cheekiralla and Engels, 2005).

6.2 Spatial identifiers – GPS

Such networking is part of a wider technological development as fixed networks move to wireless networks, *ad hoc* networks, and meshes (Mobile Ad-Hoc Networks, or MANETs). In the latter, mobile communicating devices form *ad hoc* networks (in a peer-to-peer fashion) with nearby devices to form meshes of communication that have varying topologies. The development of these kinds of networks will facilitate the increased use of spatial annotation (e.g. leaving personal messages or information within a given space). Most technological projects exploring spatial annotation use

GPS (Global Positioning System) and the use of RFID in conjunction with GPS could allow for another layer of context-specific information.

6.3 Miniaturization and motes

In the longer term, RFID tags (with some on-board computation) and wireless sensors might become so small as to be almost invisible, constituting a kind of 'smart-dust' (Rheingold, 2005). Research is being carried out into developing computational 'motes', which combine sensors, some element of communication (RF or optical) and the ability to float, even to fly. Such motes may be used in weather front analysis, or as remote sensors from dangerous environments (e.g. outer space, nuclear power plants, oceans etc.).

6.4 Technological implications – information overload

In an information-rich, digitally connected world, where much of the knowledge and tools that we make use of are outside our heads (our 'extelligence', see Stewart and Cohen, 1997) there will be a need to develop new communication 'senses' that allow us to manage and make use of the enormous amount of information we will be confronted by. This will lead to the development and adoption of new and different types of human-computer interfaces and different ways of communicating with technology.

Indeed, part of the ubicomp vision is of seamless interaction with devices, where computers become adaptive and perceptual in their interactions with users and the environment. In addition, communication between people and devices will become implicit (taking place incidentally, whilst the user is undertaking another task) and multi-modal (using all five of our senses). See, for example, The International Journal of Human-Computer Studies' special issue on information management (Zhang, 2005). In a ubiquitous computing environment, then, the user has to be not only textually, and visually literate, but also has to have 'corporal literacy', that is, an awareness of extelligence and a working knowledge of all the senses.

CONCLUSION

As a fledgling technology RFID is starting to make an impact on the core business of F&HE. Libraries are likely to initiate most of the activity over the next five years or so, but applications within administration and research are also likely to increase. It is, as yet, unclear to what extent RFID will impact on teaching and learning other than within specialist projects and it is probably more likely that these applications will develop alongside more general ubicomp developments.

RFID has the potential to be a hugely significant technology within the ubicomp vision. However, the benefits of a pervasive computing environment are unlikely to be realised unless the technology can be trusted. Where that trust does not yet exist, or is likely to be undermined by problems that may arise as the consequence of ill-considered or malicious implementation of parts of the technological 'jigsaw', the ubicomp vision will also be negatively affected. The F&HE community cannot rely on the relative ease with which RFID has so far been implemented in the UK – it is widely acknowledged that there are genuine concerns around the implementation of the technology and it would be wise for JISC to make good use of its position within the pan-European HE/ICT community to initiate a pro-active approach to developments that will impact positively on UK F&HE.

About the authors:

Gaynor Backhouse is the Project Manager of JISC TechWatch and Managing Director of Intelligent Content. Her previous experience includes managing the synthesis and dissemination of research-based material on science and new technology, and in 2002 she won an innovation award for the design of an innovative publishing technology. She is a member of the National Union of Journalists' New Media Industrial Council, which is responsible for looking at the impact of new technologies on journalism and other media-based industries.

Rob van Kranenburg lives in Ghent and works part-time in Amsterdam at Virtueel Platform, the Dutch policy organisation on e-culture. He is senior lecturer in Ambient Experience Design at the Faculty of Arts and Technology, HKU, and senior lecturer at the MA Interaction Design (EMMA). He is an external expert on the EU's Institute for Prospective Technological Studies (IPTS) project on Digital Territory – the EU vision on pervasive computing. In 2002 he edited Flow, Doors of Perception 7: the Design challenge of Pervasive Computing (www.doorsofperception.com).

Matt Ward is a Lecturer in Design at Goldsmiths College, University of London, where he runs the MA Design – Critical Practice. His research focuses on the technological construction and negotiation of social space through design. Before his post at Goldsmiths, Matt developed RFID prototypes for NCR Knowledge Lab where his research focused on designing wireless systems for domestic environments and the effects of RFID on brand identity. He has also designed and implemented locative media applications for navigating 'information space'. He holds one international patent and has a further six pending on his work. Matt has acted as research affiliate to The Auto-ID Centre, MIT Media Lab and Interaction Design department at The Royal College of Art. Matt also writes at Thinking about Things (www.triptychresearch.typepad.com).

REFERENCES

ALLAN, R. 2005. *Wireless Sensors Land Anywhere and Everywhere*. **Electronic Design**. 21st July 2005. Available online at: http://www.elecdesign.com/Articles/ArticleID/10710/10710.html [last accessed 27/03/06].

BENFORD, S. 2005. **Future location-based experiences**. JISC Technology and Standards Watch. Available at: http://www,jisc.ac.uk/techwatch [last accessed 28/03/06].

Brock, D. 2001. **The Physical Markup Language**. MIT Auto-ID Center: Cambridge, MA. Available online at: http://xml.coverpages.org/PML-MIT-AUTOID-WH-003.pdf [last accessed 28/03/06].

BROCK, D., MILNE, T., KANG, Y., LEWIS, B. 2001. **The physical markup language core components: time and place**. White Paper. Auto-ID Centre: University of Cambridge, England.

CARR, N. 2006. *The Beta Culture*. **Nicholas Carr's blog**. 11th January 2006. Available online at: http://www.roughtype.com/archives/2006/01/the_beta_cultur.php [last accessed 10/04/06].

CHEEKIRALLA, S., ENGELS, D. W. 2005. *A functional taxonomy of wireless sensor network devices*. **Proceedings of the 2nd International Conference on Broadband Networks**, pp. 26–33. IEEE.

COLLINS, 2003. *Smart Labels for Higher Education*. **RFID Journal**. 24th November 2003. http://www.rfidjournal.com/article/articleview/666/1/1/ [last accessed 10/04/06].

DEUTSCH, C., FEDER, B. 2003. *A Radio chip in every Consumer Product*. **New York Times**. 25th February 2003. The New York Times Company: USA.

DRESSEN, D. 2004. *Considerations for RFID technology selection*. **Atmel Applications journal**. Corporate communication: Atmel Corporation, iss. 3, Summer 2004.

ENGBERG, S., HARNING, M., JENSEN, C. 2004. *Zero-knowledge Device Authentication: privacy & security enhanced RFID preserving Business Value and Consumer Convenience*. **Second Annual Conference on Privacy, Security and Trust (PST)**. Available online at: http://dev.hil.unb.ca/Texts/PST/pdf/engberg.pdf [last accessed 07/04/06].

ENGELS, D.W. 2002. **A Comparison of the Electronic Product Code Identification Scheme & the Internet Protocol Address Identification Scheme.** Technical memo: Auto-ID Center. Cambridge, Massachusetts.

ENGELS, D.W., SARMA, S. E. 2005. **Standardization of requirements within the RFID class structure framework**. Technical Report: Auto-ID Center. Cambridge, Massachusetts.

European Commission, 2006. **Commission launches public consultation on radio frequency ID tags**. Press release IP/06/289: European Commission, 9th March 2006. Available online at: http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/289&format=HTML&aged=0&language=EN&guiLanguage=en [last accessed 14/04/06].

FLOERKEMEIER, C., ANARKAT, D., OSINSKI, T., HARRISON, M. 2003. **PML core specification 1.0**. Auto-ID Center Recommendation 15 September 2003. Available online at: http://www.epcglobalinc.org/standards_technology/Secure/v1.0/PML_Core_Specification_v1.0.pdf [last accessed 27/03/06].

FOGG, B. J. 2003. **Persuasive Technology: using computers to change what we think and do**. Morgan Kaufmann: USA.

GERSHENFELD, N., KRIKORIAN, R., COHEN, D. 2004. *The Internet of Things*. **Scientific American**, vol. 291, no. 4, pp. 76–78.

GILBERT, A. 2004a. *RFID chips in humans get the green light*. **Silicon.Com**. 14th October 2006. Available online at: http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39124983,00.htm [last accessed 09/04/06].

GILBERT, A. 2004b. *RFID, coming to a library near you*. **CNET news.com**. 18th October 2006. Available online at: http://news.com.com/RFID,+coming+to+a+library+near+you/2100-1012_3-5411657.html [last accessed 23/03/06].

HENNIG, J., LADKIN, P. BERND, S. 2004. Privacy enhancing technology concepts for RFID technology scrutinised. Research Report RVS-RR-04-02, 28th October 2004. University of Bielefeld: Germany. Available online at: http://www.rvs.uni-bielefeld.de/publications/Reports/PETC_RFID_Scrutinised.pdf [last accessed 12/04/06].

Hitachi. 2006. **World's smallest and thinnest RFID chip.** Press release, Hitachi Ltd: Tokyo, 6th February 2006. Available online at: http://www.hitachi.com/New/cnews/060206.html [last accessed 09/04/06].

HSI, S., FAIT, H. *RFID Enhances Visitors' museum experience at the Exploratorium*. **Communications of the ACM**. September 2005, vol. 48. no. 9. Association of Computing Machinery: USA.

HSE, 2003. **Proposal for a physical agents (electromagnetic fields) Directive**. HSE Regulatory Impact Assessment. Health and Safety Executive: London, UK. Available online at: http://www.hse.gov.uk/aboutus/hsc/meetings/2003/100603/misc11a.pdf [last accessed 14/04/06].

IDTechEx. 2005. *Active RFID: a profitable business*. **IDTechEx website**. 12th December 2005. IDTechEx Ltd: Cambridge, UK. Available online at: http://www.idtechex.com/products/en/articles/00000396.asp [last accessed 10/04/06].

IEE. 2005. **Radio Frequency Identification Device Technology (RFID) Factfile**. The Institution of Electrical Engineers. Available online at: http://www.iee.org/Policy/sectorpanels/control/rfid.cfm [last accessed 09/04/06].

International Telecommunication Union. 2005. **The Internet of Things**. ITU Internet Reports (2005) series. ITU Strategy and Policy Unit. Available online at: http://www.itu.int/osg/spu/publications/internetofthings/ [last accessed 26.03.06].

JAROSIK, M. 2005. *Short range wireless*. **M2M magazine**. January 2005.Also available online at: http://www.m2mmag.com/print/back_article.asp?ARTICLE_ID=202 [last accessed 25/03/06].

JIN-SEO, C. 2005. Multi-role MP3 player for sale. Korea Times [online]. 2nd December 2005. Available at: http://times.hankooki.com/lpage/biz/200512/kt2005120219201411910.htm [last accessed 10/04/06].

KATZ, R. N. 2005. *From tin cans to the holodeck: the future of networking in Higher Education*. IN: PIRANI, J., SALAWAY, G. 2005. **Information technology networking in Higher Education: campus commodity and competitive differentiator**. Educause Center for Applied Research (ECAR): USA.

KRIKORIAN, R., GERSHENFELD, N. 2004. *Internet 0 – inter-device internetworking*. **BT Technical Journal,** vol. 22, no. 4 (October 2004), pp. 278–284. Kluwer Academic Press: USA.

MARSTERSON, W. 2006. **TechWatch peer review**. JISC Technology and Standards Watch. JISC: Bristol.

LACE, S. 2004. **Calling in the chips?** Seminar Report. National Consumer Council: London, UK. Available online at: http://www.ncc.org.uk/technology/calling_in_chips.pdf [last accessed 12/04/06].

McFARLANE, D., SHEFFI, Y. 2003. *The Impact of Automatic Identification on Supply Chain Operations*. **The International Journal of Logistics Management**, vol. 14, no. 1. Emerald: UK.

MOROZ, 2004. Understanding Radio Frequency Identification (RFID). RMoroz.com. November 2004. Available online at: http://www.rmoroz.com/rfid.html [last accessed 14/04/06].

NAP Committee on Radio Frequency Identification Technologies. 2004. **Radio Frequency Identification Technologies: a workshop summary**. The National

Academies Press: USA. Available online at: http://www.nap.edu/catalog/11189.html [last accessed 14/04/06].

O'MALLEY, C., FRASER, D. S. 2005. *Learning with tangible technologies*. **Literature Review** series, report 12. NESTA Futurelab Publications: Bristol. Available online at: http://www.futurelab.org.uk/research/lit_reviews.htm [last accessed 14/04/06].

PARET, D. 2005. *Technical state of art of 'Radio Frequency Identification – RFID' and implications regarding standardisation, regulations, human exposure, privacy*. **Proceedings of the 2005 joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies** (sOc-EUSAI '05), pp. 9–11. ACM Press: New York, NY.

PHILIPOSE, M., FISHKIN, K., PERKOWITZ, M., PATTERSON, D., FOX, D., KAUTZ, H., HAHNEL, D. 2004. *Inferring activities from interactions with objects*. **Pervasive Computing**, vol. 3, iss. 4 (October) pp. 50–57. IEEE Educational Activities Department: USA.

PRAXIS, 2006. **Possible data objects for a library RFID system**. Book Industry Communication: London.

RFID Journal. 2006. *A summary of RFID standards*. **RFIDJournal.com**. Available online at: http://www.rfidjournal.com/article/articleview/1335/1/129/ [last accessed 09/04/06].

RFID Journal. 2003. *Military's RFID Alternative: IPv6*. **RFIDJournal.com**. Available at: http://www.rfidjournal.com/article/articleview/609/1/1/ [last accessed 23/03/06].

RHEINGOLD, H. 2002. **Smart Mobs**. Perseus Publishing: Cambridge, MA.

RIEBACK, S., CRISPO, B., TANENBAUM, A. 2006. *Is your cat infected with a computer virus?* **Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM '06)**, pp. 169–179. IEEE.

SCHMIDT, C. 2001. *Beyond the barcode*. **Technology Review**. March, 2001. MIT Press. Also available online at: http://www.schmidtwriting.com/articles/clients/tr/beyond.pdf [last accessed 11/04/06].]

STANFORD, V. 2003. *Pervasive Computing Goes the last Hundred Feet with RFID*. **Pervasive Computing**. April-June 2003, pp. 9–14. IEEE: USA. Also available online at: http://www.cs.umd.edu/~amol/course/papers/rfid03.pdf [last accessed 11/04/06].

STERLING. B. 2004. **When blobjects rule the earth**. Keynote speech: Association for Computing Machinery's Special Interest Group on Graphics and Interactive Techniques (ACM SIGGRAPH 2004), Los Angeles, August 2004. Reproduced online at: http://www.boingboing.net/images/blobjects.htm [last accessed 14/04/06].

STEWART, I., COHEN, J. 1997. **Figments of reality: the evolution of the curious mind**. Cambridge University Press: UK.

SYNTHESIS, 2004. *EPC: Electronic Product Code – the new generation RFID based product identification system.* **Synthesis Journal**. Section 3, 2004. Information Technology Standards Committee: Singapore. Available online at: http://www.itsc.org.sg/synthesis/2004/3_EPC.pdf [last accessed 11/04/06].

THOMPSON, D. 2006. *RFID technical tutorial*. **The Journal of Computing Sciences in Colleges**, vol. 21, no. 5, pp. 8–9. Consortium for Computing Sciences in Colleges: USA.

TRAUB, K., ALLGAIR, G., BARTHEL, H. et al. 2005. **The EPCglobal Architecture Framework**. EPCglobal. Available online at: http://www.epcglobalinc.org/standards_technology/Final-epcglobal-arch-20050701.pdf [last accessed 07/04/06].

Using RFID. 2005. *ID tags could help spot bird flu.* **UsingRFID.com**. 8th December 2005. Available at: http://www.usingrfid.com/news/read.asp?lc=q95777tx597zq (registration required) [last accessed 10/04/06].

WANT, R. 2004. *The magic of RFID.* **ACM Queue**, vol. 2, no. 7 (October). Association for Computing Machinery. Also available online at: http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=216 [last accessed 08/04/06].

WEBER, T. 2004. *The future of shopping*. **BBC News** [online]. 18th May 2004. Available at: http://news.bbc.co.uk/2/hi/business/3712261.stm [last accessed 10/04/06].

WEXLER, J. 2005. *Rockford Memorial to save big with Wi-Fi tracking: Hospital lassos assets with Wi-Fi net*. **Network World** [online]. 19th October 2005. Available online at: http://www.networkworld.com/newsletters/wireless/2005/1017wireless2.html [last accessed 14/04/06].

WILLIS, S., HELAL, A. 2005. *RFID Information Grid and Wearable Computing Solution to the Problem of Wayfinding for the Blind User in a Campus Environment.* **Proceedings of the ninth annual IEEE International Symposium on Wearable Computers**, Osaka, Japan, October 2005.

Also available online at: http://www.harris.cise.ufl.edu/projects_A_drishti.htm [last accessed 11/04/06].

ZHANG, D. P. (ed.) 2005. **International Journal of Human-Computer Studies**, special issue: HCI and MIS, vol. 59, iss. 4. Elsevier: Netherlands.